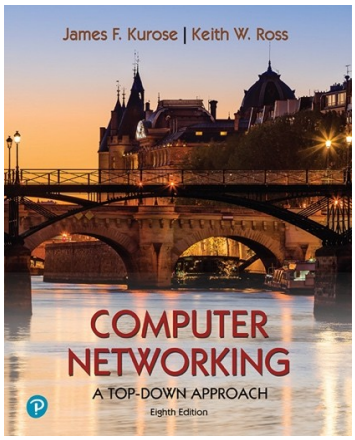
WSA 7:
Ethernet and ARP v8.1



Supplement to *Computer Networking: A Top-Down Approach, 8th ed.,* J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

You will analyze the Ethernet protocol and the ARP protocol at the Link Layer for this assignment. As this WSA concerns the Ethernet protocol and mobile devices with Wi-Fi connection is more common nowadays, **you are not asked to use Wireshark to get your own capture but use the supplied .pcap file**. Answer the questions below in your report and submit it on our ODTUClass page. While writing your report, you can cite external sources (textbook, RFCs etc.).

Since this lab is about Ethernet and ARP, we're not interested in high-level protocols like IP, TCP or HTTP. We're interested in Ethernet frames and ARP messages!

Let's start by looking at the Ethernet frame containing the HTTP **GET** message. (Recall that the HTTP GET message is carried inside of a TCP segment, which is carried inside of an IP datagram, which is carried inside of an Ethernet frame). Expand the Ethernet II information in the packet details window. Note that the contents of the Ethernet frame (header as well as payload) are displayed in the packet contents window.

1. Ethernet

1. What is the 48-bit Ethernet address of the sender?
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address?
3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? What upper layer protocol does this correspond to?
4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP **response** message.

5. What is the value of the Ethernet source address? Is this the address of the sending computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of the sender?
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame? Do not count any preamble bits in your count, i.e., assume that the Ethernet frame begins with the Ethernet frame's destination address.
9. How many Ethernet frames (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP "OK 200 ..." reply message?

2. The Address Resolution Protocol

Let's start by looking at the Ethernet frames containing ARP messages. Answer the following questions:

10. What is the hexadecimal value of the source address in the Ethernet frame containing the ARP request message sent out by the computer performing the Wireshark capture?
11. What is the hexadecimal value of the destination addresses in the Ethernet frame containing the ARP request message sent out by the sender? And what device (if any) corresponds to that address (e.g,, client, server, router, switch or otherwise...)?
12. What is the hexadecimal value for the two-byte Ethernet Frame *type* field. What upper layer protocol does this correspond to?

Answer the following question about the ARP request message sent by the computer performing the Wireshark capture.

13. How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
14. Does the ARP request message contain the IP address of the sender? If the answer is yes, what is that value?
15. What is the IP address of the device whose corresponding Ethernet address is being requested in the ARP request message sent by the sender?

Now find the ARP reply message that was sent in response to the ARP request.

16. What is the value of the *opcode* field within the ARP reply message received by the computer performing the capture?

17. Let's look at the **answer** to the ARP request message, what is the Ethernet address corresponding to the IP address that was specified in the ARP request message sent by the computer performing the Wireshark capture?
18. We've looked the ARP request message sent by the computer running Wireshark, and the ARP reply message sent in response. But there are other devices in this network that are also sending ARP request messages that you can find in the trace. Why are there no ARP replies in the trace that are sent in response to these other ARP request messages?

3. Notes

Upload your report <student_ID>.pdf to our ODTUClass page. Feel free to ask questions through ODTUClass discussions. This includes any homework question you find ambiguous. Ask for clarification rather than going with your assumption. See the course syllabus for the late submission policy. This is an individual assignment. Using any piece of code, discussion, explanation etc. that is not your own is strictly forbidden and constitutes as cheating. This includes friends, previous homework, or the Internet. The violators will be punished according to the department regulations. Please ensure that the screenshots you include in your report are legible. Answers without explanations or screenshots to support them (e.g. answering just "3" to a "how many?" question) will get no grade.